УДК 004.45, 004.89, 681.3

С.В. Гладыш
Одесская национальная академия связи, г. Одесса, Украина
sgladex@ya.ru

Иммунокомпьютинг в управлении инцидентами информационной безопасности

Исследование связано с проблемой повышения эффективности управления инцидентами информационной безопасности в инфокоммуникационных и социотехнических системах. Цель статьи – предложение нового подхода к управлению инцидентами на базе иммунокомпьютинга. Результатами исследования являются: выделенные целевые характеристики иммунной системы; обоснование подхода через метод индукции и обобщенную модель управления инцидентами; структура и функции иммунной мультиагентной системы управления инцидентами информационной безопасности.

Введение

Ощутимым проявлением проблемы инфомационной безопасности (ИБ) является факт наличия зарегистрированных и возникновения новых **инцидентов**. Причем наблюдаемый с 1998 г. по настоящее время рост числа инцидентов ИБ [1], заставляет задуматься о поиске новых, кардинальных, более эффективных и, возможно, **нестандартных** путей решения задачи управления инцидентами ИБ.

Начиная с 70-х гг. XX века были созданы и продолжают совершенствоваться теоретические исследования [2], [3], объясняющие естественные принципы и механизмы, лежащие в основе иммунитета, а также их математические модели [4], [5]. В журнале **«Искусственный интеллект»** была статья [6], посвященная одной из таких моделей. Хотя вследствие некоторых пробелов в понимании механизмов имунного ответа и межклеточных взаимодействий на сегодня отсутствует единая теория иммунитета, тем не менее теоретические предпосылки биофизических и медицинских исследований послужили толчком к возникновению нового направления в информатике – **иммунокомпьютинга**. Это дало возможность синтезировать прототипы **искусственных иммунных систем** (ИИС) для практических приложений [7].

Одним из активно исследуемых приложений ИИС является **защита информации**, где естественная иммунная система (ИС) рассматривается как источник идей и методов решения задач ИБ. Опираясь на [5] и сделав поиск по ряду научных порталов Internet, на сегодня можно выделить два общих поднаправления исследований ИИС для ИБ: 1) иммунные системы обнаружения вторжений, на базе алгоритма отрицательного отбора; 2) иммунные системы распознавания новых компьютерных вирусов.

Однако нерешенными остаются вопросы применения иммунного подхода для автоматизации и интеллектуализации процессов **управления инцидентами ИБ**.

Целью настоящего исследования является предложение нового подхода к управлению инцидентами ИБ, построенного по принципу биоаналогии на базе ИИС.

Задачи, решаемые в исследовании: обоснование междисциплинарного подхода к управлению инцидентами; построение обобщенной модели управления инцидентами; определение требований и функций управления инцидентами ИБ; синтез структуры ИИС для управления инцидентами ИБ.

Методы исследования: метод индукции (общенаучное обобщение), теория систем, эволюционный подход, интеллектуальная обработка данных, иммунокомпьютинг, агентно-ориентированный подход (мультиагентные системы).

Парадигма искусственной иммунной системы

Согласно [8] все биологические системы на уровне клеток и молекул могут рассматриваться как системы обработки информации. Но только нервная и иммунная системы обладают исключительными способностями к интеллектуальной обработке информации, включая механизмы распознавания, идентификации, принятия решений в условиях неопределенности, обучения и ассоциативной памяти [5]. По мнению некоторых ученых [4] ИС у позвоночных животных сложнее, чем нервная система.

ИС представляет собой высокопараллельную распределённую децентрализованную систему временных коллективов клеток (В-, Т-лимфоцитов, макрофагов, фагоцитов, лимфокинов и др. [3]), способную к адаптивной интеллектуальной обработке информации [4]. На данном этапе исследования ограничимся лишь рассмотрением основной способности ИС [7]: распознавать как своих или чужих огромное количество молекулярных структур – антигенов с дальнейшей их классификацией и стимуляцией соответствующих защитных механизмов. При этом результатом распознавания является обучение и формирование памяти к антигену. Знания о схожих антигенах используются при реакции на новые инфекции. Так ИС создает, совершенствует и использует знания об окружающем мире. Реакция на антиген может происходить не только на уровне отдельных распознающих единиц, но и на общесистемном уровне (в зависимости от уровня серьезности и способа проникновения инфекции [3]). Локальные взаимодействия определяют и реализуют глобальную иммунную реакцию, что в совокупности с непрерывной изменчивостью и адаптивностью иммунной памяти к частоте и силе антигенных сигналов является примером эффективной защиты при ограниченных ресурсах.

Подчеркнем аналогию функций естественной ИС с основными функциями, которые должна выполнять система управления инцидентами ИБ:

– регистрация, выявление и оценка серьезности событий, имеющих признаки инцидента, на ранних стадиях их реализации, сбор доказательств (улик) для последующего расследования;

– идентификация инцидента на основе оперативного анализа доказательств, принятие решения в условиях не полной определенности имеющейся информации и при необходимости генерация сигнала тревоги;

– обработка и устранение последствий инцидента путем введения в действие соответствующих ресурсов безопасности.

Обоснование междисциплинарного подхода

Междисциплинарный подход к решению задачи управления инцидентами (ИБ) обоснуем **методом индукции** через сопоставление и обобщение фактов возникновения инцидентов информационных процессов, которые имеют место **в системах самой разной природы** от инфокоммуникационных (ИКС) и социотехнических (СТС) до биологических [8-14].

По последним представлениям ряда различных научных направлений, таких, как социотехническая инженерия ИБ в СТС [9], защита и оценка информации в ИКС [10], теория информации [11], теоретическая физика [12], математическая биофизика и биоинформатика [8], эволюционная теория, коэволюция и ноосферогенез [13], [14] – **информация, вещество** и **энергия** составляют основу всех наблюдаемых процессов в системах самых различных уровней. К такому же заключению более 100 лет назад пришел Менделеев [15], ставя при этом именно **информационные процессы** на первом месте. В подтверждение этому в исследовании [16] формально доказано, что **информационное обеспечение** в любой системе, которая имеет цель, является важнейшим условием эффективного функционированиия.

Иммунокомпьютинг применительно к управлению инцидентами ИБ в ИКС и СТС будем реализовывать с учетом постулатов эволюционной теории [13], [14]:
- целесообразность: «выживают» лишь те ИКС/СТС, которые в наибольшей степени соответствуют ситуации, то есть приспосабливаются к инцидентам;
- адаптация: архитектура комплексной системы информационной безопасности (КСИБ) должна позволять динамически адаптироваться к новым инцидентам;
- самоорганизация: процесс эволюции ИКС/СТС приводит к непрерывному совершенствованию ее структуры в связи с перераспределением ресурсов.

Проведем междисциплинарную декомпозицию свойства безопасности абстрактной системы и взаимосвязанных с ним понятий, а также процессов управления и обработки инцидентов для следующих типов (уровней) систем: биологических, ИКС, СТС. Задача управления инцидентами в абстрактной системе является недостаточно формализованной и недоопределенной с точки зрения четкой структуры терминов ввиду недостаточной разработки более общей (по сравнению с классической) теории систем. Применив аппарат теории систем, получим следующую цепочку определений.

Под **системой** будем понимать целое, составленное из множества элементов, находящихся в отношениях и связях друг с другом, образующие определенную целостность, единство. Вследствие закона эволюционного выживания именно внешние вызовы и угрозы безопасности являются причиной образования систем, ограждающих входящие в их состав элементы от угроз различного характера.

С позиции междисциплинарного подхода под **безопасностью** будем понимать состояние защищенности системы от внешних и внутренних угроз. Угроза безопасности – совокупность условий, факторов, создающих опасность для системы (риск не превышает допустимый уровень). Состояние – мгновенное отражение системы, определяемое через характеристики входных воздействий, выходных сигналов и ее элементов. Поведение – способность системы переходить из одного состояния в другое. Равновесие (гомеостаз) – способность системы в отсутствии внешних возмущающих воздействий сохранять свое состояние сколь угодно долго.

Инцидент – событие, состоящее в реализации угрозы и выходе системы из состояния равновесия. Устойчивость – способность системы возвращаться в состояние равновесия после инцидента.

Процесс управления инцидентами – процесс *регистрации* информации о состоянии безопасности и равновесия (гомеостаза) системы, передача ее в пункты накопления и переработки, анализ поступающей, накопленной и справочной информации, принятие решения о *реагировании* на основе выполненного анализа, выработка соответствующего управляющего воздействия и доведение его до объекта управления (*обработка инцидента*).

Обобщенная модель управления инцидентами

Применяя формализм теории систем [18], построим обобщенные модели систем, соответствующие типам (уровням).

1. Для биологических систем:

$$BioSys = (GN, EC, MB, EV, FC, RP), \quad (1)$$

где GN – генетическое начало; EC – условия существования; MB – метаболизм; EV – эволюция; FC – функционирование; RP – репродукция.

2. Для инфокоммуникационных систем:

$$ICSys = (IR, EN, TR, CN, QS, SV), \quad (2)$$

где IR – информационные ресурсы; EN – среда; TR – телекоммуникационные ресурсы; CN – контроль, эксплуатация, проектирование; QS – качество; SV – надежность.

3. Для социотехнических систем:

$$STSys = (RI, RO, EX, MN, EF, ED), \quad (3)$$

где RI – внутренние ресурсы; RO – внешние ресурсы; EX – исполнители; MN – менеджмент, реинжиниринг; EF – эффекты; ED – образование, передача знаний.

Параметры GN, IR, RI представляют собой «входные сигналы» каждой из систем:
EC, EN, RO – непредсказуемые «помехи» (внешние факторы и угрозы);
MB, TR, EX – «операторы преобразования» (внутренние процессы);
EV, CN, MN – «обратная связь» (процессы внутреннего развития и самоорганизации);
FC, QS, EF – «сигнал на выходе» каждой из систем (критерии эффективности, «целевые» процессы);
RP, SV, ED – «замыкание цикла» (воспроизводство, обеспечение перехода к следующим эпохам жизни систем, «новый виток спирали»).

Можно отметить параллели между параметрами моделей каждой из систем. Это подтверждает справедливость предложенного академиком Н.Н. Моисеевым «*организмического подхода*» [13], [14] к развитию природы и общества.

Почти об этом же речь идет в исследованиях [18], [19], где показано, что проблема защиты информации с точки зрения онтологии предметной области и метамоделей представления знаний структурно подобна проблеме защиты биологических организмов от патогенных факторов.

Развивая применительно к цели настоящего исследования принцип биоаналогии и согласно метафоре «*организмического подхода*», **система управления инцидентами ИБ**, включая подсистему выявления вторжений (IDS) в рамках комплексной системы информационной безопасности (КСИБ) в ИКС или СТС, **должна играть ту же роль, что и иммунная система** (ИС) в живом организме (у позвоночных).

Применительно к управлению инцидентами ИБ это должно означать переход от «механицизма» к биологической аналогии, когда ИТС понимается как развивающаяся система, рассматриваемая сквозь призму эволюционной теории.

Теперь построим **обобщенную модель системы управления инцидентами**:

$$IMSys = (INC, SEC, CRI, KBS, X, Y, S, DMF, AGT, ARS, TRS, IRS, MST, T, SYN), \quad (4)$$

где INC –управление инцидентами (проблема); SEC – безопасность (цель); CRI – критерии оценки состояния безопасности;

KBS – база знаний об инцидентах; *X* – входные воздействия; *Y* – реакция на инцидент; *S* – состояния системы; *DMF* – функция принятия решений (реагирования); *AGT* – агенты; *ARS* – ресурсы ИБ, доступные агентам; *TRS* – пробные наборы ресурсов; *IRS* – инцидентно-ориентированные наборы ресурсов; *MST* – стратегия управления инцидентами; *T* – время; *SYN* – самоорганизация.

Подробнее поясним некоторые введенные понятия:

AGT – множество программно реализованных мобильных интеллектуальных агентов;

ARS – агентно-ориентированный набор ресурсов безопасности, то есть множество всех доступных для агентов ресурсов безопасности;

IRS – инцидентно-ориентированный набор ресурсов безопасности, то есть подмножество ресурсов, которыми располагают агенты и которое в совокупности является достаточным для эффективного реагирования на конкретный тип инцидента;

TRS – пробный (тестовый) набор ресурсов безопасности, то есть подмножество ресурсов, которые отбираются для имитационного моделирования, прогноза и адаптации к неизвестному типу инцидента.

DMF – функция, которая включает два подэтапа: принятие решения о включении элемента *ARS* в набор *TRS* и затем на основании первого подэтапа – принятие решения о включении элемента *ARS* в набор *IRS*.

Иммунная система управления инцидентами ИБ

Непременным свойством любой системы является наличие **структуры**, которая представляет собой построение системы, отражающее наиболее существенные взаимосвязи между элементами и их группами (подсистемами), которые мало меняются при изменениях в системе и обеспечивают устойчивое существование системы и ее основных свойств.

В сетевой и организационной архитектуре ИКС/СТС выделим подсистему автоматизированного управления инцидентами ИБ (рис. 1).

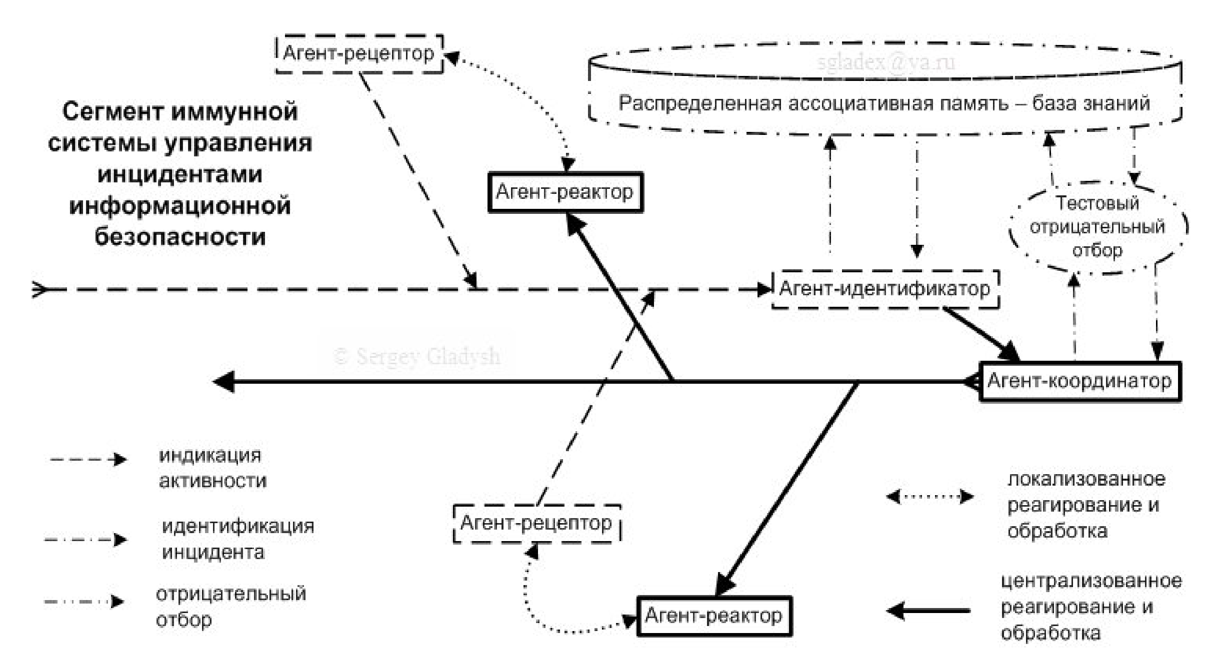


Рисунок 1 – Структура иммунной мультиагентной системы управления инцидентами ИБ

Будем проектировать данную систему, используя иммуно-мультиагентную технологию [19]. Рассмотрим 4 класса агентов (рис. 2): агенты-детекторы; агенты-идентификаторы; агенты-координаторы; агенты-реакторы.

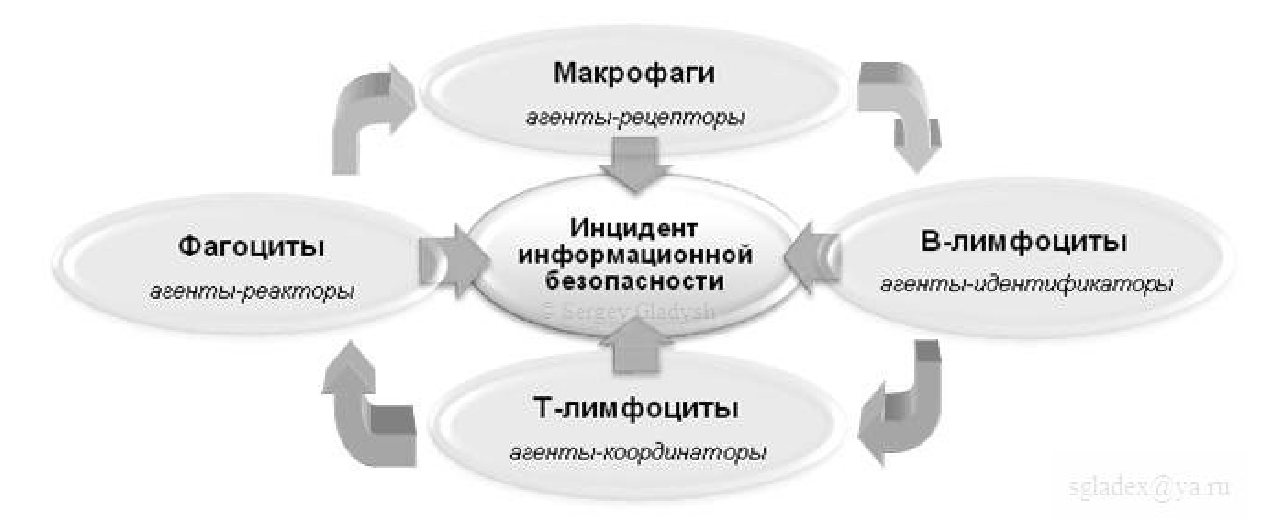


Рисунок 2 – Цикл и функции управления инцидентами посредством ИИС

Агенты-детекторы соответствуют макрофагам и другим антиген-презентирующим клеткам, которые выставляют частицы антигена на своей поверхности, привлекая внимание В-лимфоцитов для распознавания. Агенты-идентификаторы соответствуют В-лимфоцитам, которые распознают антиген и заранее подвергались «отрицательному отбору» в тимусе. Агенты-координаторы соответствуют лимфокинам, выделяемым Т-лимфоцитами для активации В-лимфоцитов. Агенты-реакторы соответствуют фагоцитам, имеющим антитела для уничтожения антигена.

Выделим следующие этапы управления инцидентами с помощью ИИС:

1) индикация агентами-детекторами любой подозрительной активности;

2) распознавание агентами-идентификаторами ненормальной активности как определенного типа инцидента при условии нахождения в базе знаний соответствующей сигнатуры или выявление аномалии по отношению к эталону поведения;

3) получение подсистемой реагирования сигнала от IDS об идентифицированном известном или неизвестном инциденте;

4) идентификация атакующего набора угроз инцидента при условии наличия в базе знаний корреляции между характеристиками полученного сигнала об инциденте и записями о наборах атакующих угроз;

5) формирование тестовых наборов механизмов защиты согласно алгоритму, который генерируется базой знаний;

6) имитационное моделирование эффективности перекрытия тестовым набором механизмов защиты – набора атакующих угроз конкретного идентифицированного инцидента;

7) принятие решения относительно выбора инцидентно-ориентированного набора механизмов защиты;

8) выдача подсистемой обработки управляющего сигнала агентам-реакторам относительно обработки инцидента с помощью инцидентно-ориентированного набора механизмов защиты;

9) самоорганизация и оценка подсистемой обратной связи и агентами-детекторами эффективности использования инцидентно-ориентированного набора механизмов защиты, пополнение баз знаний новым опытом, расследование и анализ инцидента, выработка управляющего сигнала относительно превентивных действий.

Для того, чтобы составить единый организм, агенты должны обеспечивать гомеостатическое регулирование ИКС/СТС в целом. Под гомеостатическим регулированием понимается управление инцидентами, поддерживающее целевые характеристики ИКС/СТС, в пределах, обеспечивающих ее безопасность, качество, надёжность и живучесть.

Выводы

В ходе исследования были получены новые научно-теоретические результаты: впервые предложен, логически обоснован и математически формализован иммунный подход к интеллектуальному управлению инцидентами ИБ в ИКС и СТС, построена обобщенная модель управления инцидентами. Показана практическая целесообразность и прикладное значение полученных результатов на примере разработки прототипа структуры и функций иммунной системы управления инцидентами ИБ на базе агентно-ориентированного подхода к построению распределенных программных систем. Данный подход обеспечивает динамическое адаптивное управление при возникновении новых инцидентов. Применение ИИС в автоматизации и интеллектуализации управления инцидентами ИБ может позволить достичь качественно нового уровня обеспечения и управления ИБ в ИКС и СТС.

Литература

1. Howard J. An Analysis of Security Incidents in the Internet. – CERT/CC, 2000.
2. Jerne N.K. The immune system // Sci. Am. – 1973. – Vol. 229, № 1. – P. 52-60.
3. Петров Р.В. Иммунология. – М.: Медицина, 1987. – 416 с.
4. Perelson A.S. Immune network theory // Immunol. Rev. – 1989. – Vol. 10. – P. 5-36.
5. Марчук Г.И. Математические модели в иммунологии. Вычислительные методы и эксперименты. – М.: Наука, 1991. – 304 с.
6. Марценюк В.П. Исследование характеристик нелинейной динамики и хаоса в модели противоопухолевого иммунитета // Искусственный интеллект. – 2004. – № 3.
7. Искусственные иммунные системы и их применение: Пер. с англ. / Под ред. Д. Дасгупты. – М.: Физматлит, 2006. – 344 с.
8. Романовский Ю.М., Степанова Н.В., Чернавский Д.С. Математическая биофизика. – М.: Наука, 1984.
9. Остапенко Г.А. Информационные операции и атаки в социотехнических системах. – М.: Горячая линия – Телеком, 2007. – 134 с.
10. Бугров Ю.Г. Системные основы оценивания и защиты информации. – Воронеж: ВГТУ, 2005. – 354 с.
11. Чернавский Д.С. Синергетика и информация (динамическая теория информации). – 2-е изд. – М.: Эдиториал УРСС, 2004. – 288 с.
12. Хакен Г. Информация и самоорганизация. Макроскопический подход к сложным системам: Пер. с англ. – М.: Мир, 1991. – 240 с.
13. Моисеев Н.Н. Универсальный эволюционизм и коэволюция // Природа. – 1989. – № 4. – С. 3-8.
14. Моисеев Н.Н. Коэволюция природы и общества. Пути ноосферогенеза // Экология и жизнь. – 1997. – № 2.
15. Менделеев Д.И. Заветные мысли. – М.: Мысль, 1995. – 414 с.
16. Акофф Р., Эмери Ф. О целеустремленных системах: Пер. с англ. – М.: Сов. радио, 1974. – 272 с.

17. Компьютерная поддержка сложных организационно-технических систем / Борисов В.В., Бычков И.А., Дементьев А.В., Соловьев А.П., Федулов А.С. – М.: Горячая линия – Телеком, 2002.
18. Гладыш С.В. Применение принципа биоаналогии для синтеза систем интеллектуального управления безопасностью телекоммуникаций // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. – 2006. – № 13. – С. 57-63.
19. Гладыш С.В. Принцип биологической и медицинской аналогии в моделях представления знаний систем интеллектуального управления безопасностью телекоммуникаций // Сб. матер. IV Междунар. науч.-практ. конфер. «Информационные технологии и кибернетика на службе здравоохранения». – Днепропетровск: ИТМ. – 2006. – С. 21-24.
20. Gladysh S.V. A multi-agent immune approach to information security assurance in telecommunications // Сб. матер. IV Междунар. науч.-техн. конфер. «Мир информации и телекоммуникаций – 2007». – Киев: ГУИКТ. – 2007. – С. 113.

С.В. Гладиш

Імунокомп'ютинг в керуванні інцидентами інформаційної безпеки

Дослідження пов'язане з проблемою підвищення ефективності керування інцидентами інформаційної безпеки в інфокомунікаційних та соціотехнічних системах. Мета статті – пропозиція нового підходу до керування інцидентами на базі імунокомп'ютингу. Результатами дослідження є: виділені цільові характеристики імунної системи; обґрунтування підходу через метод індукції та узагальнену модель керування інцидентами; структура й функції імунної мультиагентної системи керування інцидентами інформаційної безпеки.

S.V. Gladysh

Immunocomputing in Information Security Incident Management

The research concerns efficiency improving of information security incidents management in infocommunication and socio-technical systems. The goal is to propose a new immunologically-inspired approach to incidents management. The results of the research are: the focused target properties of immune systems; the approach proof by the induction and the generalized model of incidents management; the structure and functions of an immune multi-agent system for information security incidents management.

Статья поступила в редакцию 25.12.2007.